

Title (en)

BLOCKCHAIN-BASED IDENTITY AUTHENTICATION METHOD, DEVICE, NODE AND SYSTEM

Title (de)

BLOCKCHAIN-BASIERTES IDENTITÄTSAUTHENTIFIZIERUNGSVERFAHREN, VORRICHTUNG, KNOTEN UND SYSTEM

Title (fr)

PROCÉDÉ, DISPOSITIF, NOEUD ET SYSTÈME D'AUTHENTIFICATION D'IDENTITÉ FONDÉS SUR UNE CHAÎNE DE BLOCS

Publication

**EP 3486817 A4 20190911 (EN)**

Application

**EP 16916036 A 20160918**

Priority

CN 2016099254 W 20160918

Abstract (en)

[origin: EP3486817A1] The present disclosure discloses a method, apparatus, node, system for blockchain-based identity authentication, and relates to the field of security technology. The method includes: receiving an authentication request sent by an authenticated party node, wherein the authentication request includes the identity information of the authenticated party node and the identity information of an identity proof publishing node; in the case that it is determined that the information and a digital signature of the identity proof publishing node on the identity information of the authenticated party node have been written into a blockchain, verifying the digital signature according to a public key of the identity proof publishing node; after the digital signature passes the verification, determining whether the authenticated party node has mastered a private key corresponding to the public key of the authenticated party node, wherein the public key of the authenticated party node is obtained according to the identity information of the authenticated party node; and in the case that it is determined that the authenticated party node has mastered the private key corresponding to the public key of the authenticated party node, it is determined that the authenticated party node passes the identity authentication.

IPC 8 full level

**G06F 21/31** (2013.01); **H04L 9/32** (2006.01); **H04L 29/06** (2006.01)

CPC (source: CN EP US)

**G06F 21/33** (2013.01 - EP US); **G06F 21/64** (2013.01 - EP US); **H04L 9/0637** (2013.01 - US); **H04L 9/0891** (2013.01 - EP US); **H04L 9/30** (2013.01 - US); **H04L 9/3218** (2013.01 - US); **H04L 9/3239** (2013.01 - EP US); **H04L 9/3247** (2013.01 - CN EP US); **H04L 9/50** (2022.05 - EP); **H04L 63/08** (2013.01 - CN EP US); **H04L 9/50** (2022.05 - US)

Citation (search report)

- [A] US 2016162897 A1 20160609 - FEENEY PATRICK JOSEPH [US]
- [A] KR 101637854 B1 20160708 - COINPLUG LNC [KR] & US 2019005470 A1 20190103 - UHR JOON SUN [KR], et al
- [A] CONNER FROMKNECHT ET AL: "A Decentralized Public Key Infrastructure with Identity Retention", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH., vol. 20141111:124302, 6 October 2014 (2014-10-06), pages 1 - 16, XP061017076
- See references of WO 2018049656A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

**EP 3486817 A1 20190522; EP 3486817 A4 20190911; EP 3486817 B1 20201111**; CN 107079037 A 20170818; CN 107079037 B 20181023; JP 2019519987 A 20190711; JP 6684930 B2 20200422; US 10581615 B2 20200303; US 2019288854 A1 20190919; WO 2018049656 A1 20180322

DOCDB simple family (application)

**EP 16916036 A 20160918**; CN 2016099254 W 20160918; CN 201680003232 A 20160918; JP 2018561592 A 20160918; US 201616318284 A 20160918